CLAIMS

What is claimed is:

1. An apparatus comprising:

a translation lookaside buffer (TLB) in a processor having a plurality of TLB entries, each TLB entry being associated with a virtual machine extension (VMX) tag word indicating if the associated TLB entry is invalidated according to the processor mode when an invalidation operation is performed, the processor mode being one of execution in a virtual machine (VM) and execution not in a virtual machine, the invalidation operation belonging to a non-empty set of invalidation operations composed of a union of (1) a possibly empty set of operations that invalidate a variable number of TLB entries, (2) a possibly empty set of operations that invalidate exactly one TLB entry, (3) a possibly empty set of operations that invalidate the plurality of TLB entries, (4) a possibly empty set of operations that enable and disable use of virtual memory, and (5) a possibly empty set of operations that configure physical address size, page size or other virtual memory system behavior in a manner that changes the manner in which a physical machine interprets the TLB entries.

2. The apparatus of claim 1 wherein the invalidation operation is one of (1) a loading of a first control register conditioned on a global bit, (2) an execution of a page invalidate instruction, (3) a task switch that modifies the first control register, (4) a loading of a second control register that modifies one of a protected mode indicator and a page mode indicator, and (5) a loading of a third control register that modifies one of a page size extension (PSE), a page global enable (PGE), and a physical address extension (PAE).

3. The apparatus of claim 2 wherein the processor is in or not in VMX mode [e1]and the TLB entry is not invalidated at loading of the first control

register when one of a transition into VMX mode (a VM entrance) and a transition out of VMX mode (a VM exit) occurs.

4. The apparatus of claim 3 wherein the VMX tag word is a single bit and

the VMX tag word is negated for a new TLB entry when the processor is not in VMX mode and the VMX tag word is asserted for a new TLB entry when the processor is in VMX mode; and

the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word is asserted and the processor is in VMX mode.

5. The apparatus of claim 4 wherein the TLB entry is invalidated irrespective of value of the VMX tag word when an invalidation operation is performed and the processor is not in VMX mode.

6. The apparatus of claim 4 wherein a field in a control register is designated the translation lookaside buffer virtual machine extension (TLBVMX) word and the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word matches the TLBVMX word and the processor is not in VMX mode.

7. The apparatus of claim 3 wherein the VMX tag word is a single bit and

the VMX tag word is asserted for a new TLB entry when the processor is not in VMX mode and the VMX tag word is negated for a new TLB entry when the processor is in VMX mode; and

the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word is negated and the processor is in VMX mode.

8. The apparatus of claim 7 wherein the TLB entry is invalidated irrespective of the value of the VMX tag word when an invalidation operation is performed and the processor is not in VMX mode.

9. The apparatus of claim 7 wherein a field in a control register is designated the TLBVMX word and the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word matches the TLBVMX word and the processor is not in VMX mode.

10. The apparatus of claim 1 wherein invalidation of a TLB entry by an invalidation operation is further conditioned upon value of one or more control words associated with the TLB.

11. The apparatus of claim 10 wherein the control word or words associated with the TLB are located in one or more of the control registers of the processor or in a Virtual Machine Control Structure (VMCS) in memory.

12. The apparatus of claim 11 wherein one of the control words associated with the TLB is distinguished such that the VMX tag word is set to match a distinguished control word for a new TLB entry, the distinguished control word associated with the TLB being designated the TLBVMX word.

13. The apparatus of claim 12 wherein the TLBVMX word is set to one of a plurality of values that constitute a proper subset of a set of all possible values for a VMX tag word when the processor mode corresponds to execution in a virtual machine (VM).

14. The apparatus of claim 13 wherein the TLB entry is invalidated when an invalidation operation is performed and the value of the associated VMX

tag word matches the value of the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM).

15. The apparatus of claim 14 wherein the one or more control words associated with the TLB, including the TLBVMX word, are configurable when the processor mode corresponds to execution not in a virtual machine.

16. The apparatus of claim 13 wherein the TLBVMX word is set to one of a plurality of values that constitute a proper subset of a set of all possible values for a VMX tag word when the processor mode corresponds to execution not in a virtual machine.

17. The apparatus of claim 16 wherein a set theoretic intersection of the plurality of values allowable for the TLBVMX word when the processor mode corresponds to execution not in a virtual machine and the plurality of values allowable for the TLBVMX word when the processor mode corresponds to execution in a virtual machine (VM) is an empty set.

18. The apparatus of claim 16 wherein invalidation of a TLB entry by an invalidation operation is further conditioned upon value of a second control word associated with the TLB when the processor mode corresponds to execution not in a virtual machine.

19. The apparatus of claim 18 wherein the TLB entry is invalidated when an invalidation operation is performed and the associated VMX tag word matches the second control word associated with the TLB and the processor mode corresponds to execution not in a virtual machine.

20. The apparatus of claim 18 wherein the TLB entry is invalidated when an invalidation operation is performed and the logical AND of the

associated VMX tag word and the second control word associated with the TLB matches the TLBVMX word and the processor mode corresponds to execution in a virtual machine, the second control word associated with the TLB being designated the TLBVMX mask word.

21. The apparatus of claim 20 wherein access by software to configure a portion of the TLBVMX word when the processor mode corresponds to execution in a virtual machine (VM) is conditioned upon value of the TLBVMX mask word such that software executing when the processor mode corresponds to execution in a virtual machine (VM) is able to set the TLBVMX word to a value such that the logical AND of a new value of the TLBVMX word and a value of the TLBVMX mask word matches a logical AND of a previous value of the TLBVMX word and the value of TLBVMX mask word.

22. The apparatus of claim 21 wherein the processor maintains a stack of TLBVMX mask words such that

software executing when the processor mode corresponds to execution in a virtual machine (VM) pushes the current value of the TLBVMX mask word onto a processor-maintained stack and places a new value in the TLBVMX mask word incident to a VM entrance,

the new value of the TLBVMX mask word is logically ORed with a previous value of the TLBVMX mask word and stores the value in the TLBVMX mask word so that a logical AND of the new value and the previous value is guaranteed to equal the previous value of the TLBVMX mask word, and

a previously pushed value of TLBVMX mask word is automatically popped from the processor-maintained stack incident to a VM exit.

23. The apparatus of claim 22 wherein the TLB entry is invalidated when an invalidation operation is performed and a logical AND of the associated VMX tag word and the TLBVMX mask word matches the value of the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM).

24. The apparatus of claim 23 wherein the bits configured in the VMX tag word and the TLBVMX word are determined by the current TLBVMX mask word.

25. The apparatus of claim 24 wherein the bits configured in the VMX tag word and the TLBVMX word are determined by an execution of a specified processor instruction in a specified manner.

26. The apparatus of claim 25 wherein the execution of the specified processor instruction in the specified manner returns a value that indicates the number of bits cleared to 0 in the current TLBVMX mask word and the bits in the TLBVMX word and VMX tag words are prevented from being read or configured when the corresponding bits are set to 1 in the current TLBVMX mask word.

27. The apparatus of claim 18 wherein the TLB entry is invalidated when an invalidation operation is performed and the logical AND of the associated VMX tag word with a logical NOT of the second control word associated with the TLB matches the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM), the second control word associated with the TLB being designated the TLBVMX inverted mask word.

28. The apparatus of claim 27 wherein access by software to configure a portion of the TLBVMX word when the processor mode corresponds to execution in a virtual machine (VM) is conditioned upon the value of the TLBVMX inverted mask word such that software executing when the processor mode corresponds to execution in a virtual machine (VM) is able to set the TLBVMX word to a value such that a logical AND of a new value of the TLBVMX word and the logical NOT of the TLBVMX inverted mask word matches the logical AND of a previous value of the TLBVMX word and the logical NOT of TLBVMX inverted mask word.

29. The apparatus of claim 28 wherein the processor maintains a stack of TLBVMX inverted mask words such that

software executing when the processor mode corresponds to execution in a virtual machine (VM) pushes the current value of the TLBVMX inverted mask word onto a processor-maintained stack and places a new value in the TLBVMX inverted mask word incident to a VM entrance,

the processor automatically logically ANDs the new value of the TLBVMX inverted mask word with the previous value of the TLBVMX mask word and stores the value in the TLBVMX mask word so that the logical OR of the new value and the previous value is guaranteed to equal the previous value of the TLBVMX mask word, and

a previously pushed value of TLBVMX inverted mask word is popped from the processor maintained stack incident to a VM exit.

30. The apparatus of claim 29 wherein the TLB entry is invalidated when an invalidation operation is performed and a logical AND of the associated VMX tag word and the logical NOT of the TLBVMX inverted mask word matches the value of the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM).

31. The apparatus of claim 30 wherein the bits that software may configure in the VMX tag word and the TLBVMX word is determined by the current TLBVMX inverted mask word.

32. The apparatus of claim 31 wherein the method of determining the bits that software may configure in the VMX tag word and the TLBVMX word is to execute a specified processor instruction in a specified manner.

33. The apparatus of claim 32 wherein the executing the specified processor instruction in a specified manner returns a value that indicates the

number of bits set to 1 in the current TLBVMX inverted mask word and the processor prevents software from reading or configuring bits in the TLBVMX word and VMX tag words when the corresponding bits are cleared to 0 in the current TLBVMX inverted mask word.

34. The apparatus of claim 16 wherein size of a VMX tag word and the TLBVMX word is determined by executing a specified processor instruction in a specified manner.

35. The apparatus of claim 34 wherein the processor is compatible with the Intel Architecture and the specified instruction is a CPUID instruction and the specified manner is to have a specified value in an EAX register when the CPUID instruction is executed.

36. A method comprising:

associating a translation lookaside buffer (TLB) entry in a plurality of TLB entries in a processor with a virtual machine extension (VMX) tag word to indicate if the associated TLB entry is invalidated according to the processor mode when an invalidation operation is performed, the processor mode being one of execution in a virtual machine (VM) and execution not in a virtual machine; and

performing the invalidation operation, the invalidation operation belonging to a non-empty set of invalidation operations composed of a union of (1) a possibly empty set of operations that invalidate a variable number of TLB entries, (2) a possibly empty set of operations that invalidate exactly one TLB entry, (3) a possibly empty set of operations that invalidate the plurality of TLB entries, (4) a possibly empty set of operations that enable and disable use of virtual memory, and (5) a possibly empty set of operations that configure physical address size, page size or other virtual memory system behavior in a manner that changes the manner in which a physical machine interprets the TLB entries.

37. The method of claim 36 wherein performing comprises performing the invalidation operation being one of (1) a loading of a first control register conditioned on a global bit, (2) an execution of a page invalidate instruction, (3) a task switch that modifies the first control register, (4) a loading of a second control register that modifies one of a protected mode indicator and a page mode indicator, and (5) a loading of a third control register that modifies one of a page size extension (PSE), a page global enable (PGE), and a physical address extension (PAE).

38. The method of claim 37 wherein the processor is in or not in VMX mode [e2]and the TLB entry is not invalidated at loading of the first control register when one of a transition into VMX mode (a VM entrance) and a transition out of VMX mode (a VM exit) occurs.

39. The method of claim 38 further comprising:

negating the VMX tag word for a new TLB entry when the processor is not in VMX mode, the VMX tag word being a single bit;

asserting the VMX tag word for a new TLB entry when the processor is in VMX mode; and

invalidating the TLB entry when an invalidation operation is performed and the VMX tag word is asserted and the processor is in VMX mode.

40. The method of claim 39 wherein invalidating comprises invalidating the TLB entry irrespective of value of the VMX tag word when an invalidation operation is performed and the processor is not in VMX mode.

41. The method of claim 39 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and the VMX tag word matches the translation lookaside buffer virtual machine extension

(TLBVMX) word and the processor is not in VMX mode, the TLBVMX word designating a field in a control register.

42. The method of claim 38 further comprising:

asserting the VMX tag word for a new TLB entry when the processor is not in VMX mode, the VMX tag word being a single bit;

negating the VMX tag word for a new TLB entry when the processor is in VMX mode; and

invalidating the TLB entry when an invalidation operation is performed and the VMX tag word is negated and the processor is in VMX mode.

43. The method of claim 42 wherein invalidating comprises invalidating the TLB entry irrespective of the value of the VMX tag word when an invalidation operation is performed and the processor is not in VMX mode.

44. The method of claim 42 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and the VMX tag word matches the TLBVMX word and the processor is not in VMX mode, the TLBVMX word designating a field in a control register.

45. The method of claim 42 wherein invalidating comprises invalidating the TLB entry by the invalidation operation conditioned upon value of one or more control words associated with the TLB.

46. The method of claim 45 wherein the control word or words associated with the TLB are located in one or more of the control registers of the processor or in a Virtual Machine Control Structure (VMCS) in memory.

47. The method of claim 46 further comprising distinguishing one of the control words associated with the TLB such that the VMX tag word is set to

match a distinguished control word for a new TLB entry, the distinguished control word associated with the TLB being designated the TLBVMX word.

48. The method of claim 47 further comprising setting the TLBVMX word to one of a plurality of values that constitute a proper subset of a set of all possible values for a VMX tag word when the processor mode corresponds to execution in a virtual machine (VM).

49. The method of claim 48 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and the value of the associated VMX tag word matches the value of the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM).

50. The method of claim 49 further comprising configuring the one or more control words associated with the TLB, including the TLBVMX word, when the processor mode corresponds to execution not in a virtual machine.

51. The method of claim 48 further comprising setting the TLBVMX word to one of a plurality of values that constitute a proper subset of a set of all possible values for a VMX tag word when the processor mode corresponds to execution not in a virtual machine.

52. The method of claim 51 wherein a set theoretic intersection of the plurality of values allowable for the TLBVMX word when the processor mode corresponds to execution not in a virtual machine and the plurality of values allowable for the TLBVMX word when the processor mode corresponds to execution in a virtual machine (VM) is an empty set.

53. The method of claim 51 wherein invalidation of a TLB entry by an invalidation operation is further conditioned upon value of a second control word

associated with the TLB when the processor mode corresponds to execution not in a virtual machine.

54. The method of claim 53 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and the associated VMX tag word matches the second control word associated with the TLB and the processor mode corresponds to execution not in a virtual machine.

55. The method of claim 53 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and the logical AND of the associated VMX tag word and the second control word associated with the TLB matches the TLBVMX word and the processor mode corresponds to execution in a virtual machine, the second control word associated with the TLB being designated the TLBVMX mask word.

56. The method of claim 55 further comprising accessing by software to configure a portion of the TLBVMX word when the processor mode corresponds to execution in a virtual machine (VM) conditioned upon value of the TLBVMX mask word such that software executing when the processor mode corresponds to execution in a virtual machine (VM) is able to set the TLBVMX word to a value such that the logical AND of a new value of the TLBVMX word and a value of the TLBVMX mask word matches a logical AND of a previous value of the TLBVMX word and the value of TLBVMX mask word.

57. The method of claim 56 further comprising maintaining a stack of TLBVMX mask words by the processor such that

software executing when the processor mode corresponds to execution in a virtual machine (VM) pushes the current value of the TLBVMX mask word onto a processor-maintained stack and places a new value in the TLBVMX mask word incident to a VM entrance,

the new value of the TLBVMX mask word is logically ORed with a previous value of the TLBVMX mask word and stores the value in the TLBVMX mask word so that a logical AND of the new value and the previous value is guaranteed to equal the previous value of the TLBVMX mask word, and

a previously pushed value of TLBVMX mask word is automatically popped from the processor-maintained stack incident to a VM exit.

58. The method of claim 57 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and a logical AND of the associated VMX tag word and the TLBVMX mask word matches the value of the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM).

59. The method of claim 58 further comprising determining the bits configured in the VMX tag word and the TLBVMX word by the current TLBVMX mask word.

60. The method of claim 59 wherein determining the bits configured in the VMX tag word and the TLBVMX word comprises executing a specified processor instruction in a specified manner.

61. The method of claim 60 wherein executing the specified processor instruction in the specified manner comprises returning a value that indicates the number of bits cleared to 0 in the current TLBVMX mask word; and preventing the bits in the TLBVMX word and VMX tag words from being read or configured when the corresponding bits are set to 1 in the current TLBVMX mask word.

62. The method of claim 53 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and the logical AND of the associated VMX tag word with a logical NOT of the second control word associated with the TLB matches the TLBVMX word and the

processor mode corresponds to execution in a virtual machine (VM), the second control word associated with the TLB being designated the TLBVMX inverted mask word.

63. The method of claim 62 further comprising accessing by software to configure a portion of the TLBVMX word when the processor mode corresponds to execution in a virtual machine (VM) conditioned upon the value of the TLBVMX inverted mask word such that software executing when the processor mode corresponds to execution in a virtual machine (VM) is able to set the TLBVMX word to a value such that a logical AND of a new value of the TLBVMX word and the logical NOT of the TLBVMX inverted mask word matches the logical AND of a previous value of the TLBVMX word and the logical NOT of TLBVMX inverted mask word.

64. The method of claim 63 further comprising maintaining a stack of TLBVMX inverted mask words by the processor such that

software executing when the processor mode corresponds to execution in a virtual machine (VM) pushes the current value of the TLBVMX inverted mask word onto a processor-maintained stack and places a new value in the TLBVMX inverted mask word incident to a VM entrance,

the processor automatically logically ANDs the new value of the TLBVMX inverted mask word with the previous value of the TLBVMX mask word and stores the value in the TLBVMX mask word so that the logical OR of the new value and the previous value is guaranteed to equal the previous value of the TLBVMX mask word, and

a previously pushed value of TLBVMX inverted mask word is popped from the processor maintained stack incident to a VM exit.

65. The method of claim 64 wherein invalidating comprises invalidating the TLB entry when an invalidation operation is performed and a logical AND of the associated VMX tag word and the logical NOT of the

TLBVMX inverted mask word matches the value of the TLBVMX word and the processor mode corresponds to execution in a virtual machine (VM).

66. The method of claim 65 further comprising determining bits configured in the VMX tag word and the TLBVMX word by the current TLBVMX inverted mask word.

67. The method of claim 66 wherein determining the bits comprises determining the bits configured in the VMX tag word and the TLBVMX word by executing a specified processor instruction in a specified manner.

68. The method of claim 67 wherein the executing the specified processor instruction in a specified manner comprises returning a value that indicates the number of bits set to 1 in the current TLBVMX inverted mask word; and preventing the bits in the TLBVMX word and VMX tag words from being read or configured when the corresponding bits are cleared to 0 in the current TLBVMX inverted mask word.

69. The method of claim 51 wherein determining comprises determining size of a VMX tag word and the TLBVMX word by executing a specified processor instruction in a specified manner.

70. The method of claim 69 wherein the processor is compatible with the Intel Architecture and the specified instruction is a CPUID instruction and the specified manner is to have a specified value in an EAX register when the CPUID instruction is executed.

71. A processor comprising:

a translation lookaside buffer (TLB) having a plurality of TLB entries, each TLB entry being associated with a virtual machine extension (VMX) tag word indicating if the associated TLB entry is invalidated according to the

processor mode when an invalidation operation is performed, the processor mode being one of execution in a virtual machine (VM) and execution not in a virtual machine, the invalidation operation belonging to a non-empty set of invalidation operations composed of a union of (1) a possibly empty set of operations that invalidate a variable number of TLB entries, (2) a possibly empty set of operations that invalidate exactly one TLB entry, (3) a possibly empty set of operations that invalidate the plurality of TLB entries, (4) a possibly empty set of operations that enable and disable use of virtual memory, and (5) a possibly empty set of operations that configure physical address size, page size or other virtual memory system behavior in a manner that changes the manner in which a physical machine interprets the TLB entries; and

first, second, and third registers coupled to the TLB to store information related to the invalidation operation.

72. The processor of claim 71 wherein the invalidation operation is one of (1) a loading of the first control register conditioned on a global bit, (2) an execution of a page invalidate instruction, (3) a task switch that modifies the first control register, (4) a loading of the second control register that modifies one of a protected mode indicator and a page mode indicator, and (5) a loading of the third control register that modifies one of a page size extension (PSE), a page global enable (PGE), and a physical address extension (PAE).

73. The processor of claim 72 wherein the processor is in or not in VMX mode and the TLB entry is not invalidated at loading of the first control register when one of a transition into VMX mode (a VM entrance) and a transition out of VMX mode (a VM exit) occurs.

74. The processor of claim 73 wherein the VMX tag word is a single bit and

the VMX tag word is negated for a new TLB entry when the processor is not in VMX mode and the VMX tag word is asserted for a new TLB entry when the processor is in VMX mode; and

the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word is asserted and the processor is in VMX mode.

75. The processor of claim 74 wherein the TLB entry is invalidated irrespective of value of the VMX tag word when an invalidation operation is performed and the processor is not in VMX mode.

76. The processor of claim 74 wherein a field in a control register is designated the translation lookaside buffer virtual machine extension (TLBVMX) word and the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word matches the TLBVMX word and the processor is not in VMX mode.

77. The processor of claim 73 wherein the VMX tag word is a single bit and

the VMX tag word is asserted for a new TLB entry when the processor is not in VMX mode and the VMX tag word is negated for a new TLB entry when the processor is in VMX mode; and

the TLB entry is invalidated when an invalidation operation is performed and the VMX tag word is negated and the processor is in VMX mode.

78. The processor of claim 77 wherein the TLB entry is invalidated irrespective of the value of the VMX tag word when an invalidation operation is performed and the processor is not in VMX mode.

79. The processor of claim 77 wherein a field in a control register is designated the TLBVMX word and the TLB entry is invalidated when an

invalidation operation is performed and the VMX tag word matches the TLBVMX word and the processor is not in VMX mode.

80. - The processor of claim 71 wherein invalidation of a TLB entry by an invalidation operation is further conditioned upon value of one or more control words associated with the TLB.